

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

- 1                   1-27. (Canceled)
- 1                   28. (Previously presented): The method of claim 30, further comprising the  
2 step of:  
3                   providing ingress filtering at said logical ports.
- 1                   29. (Previously presented): The method of claim 30, wherein said security  
2 association contains at least two keys, one key for encryption and another key for computing an  
3 authentication code, wherein said security association is associated with a VLAN, wherein said  
4 authentication code is used to limit traffic at one of said logical ports to members of an entire  
5 VLAN, wherein encryption is used to keep traffic private except to members, wherein only  
6 stations having said security association belong to said VLAN, and wherein all stations having  
7 said security association belong to the same broadcast domain.
- 1                   30. (Previously presented): The method of claim 31, wherein said access  
2 point may serve more than one VLAN by having multiple logical ports associated with it.
- 1                   31. (Currently amended): In a system for segregating traffic amongst a  
2 plurality of stations that are associated with an access point, a method for joining a personal  
3 virtual local area network (VLAN) served by said access point, comprising steps of:  
4                   providing a control channel for authentication of a requester by a creator of said  
5 personal VLAN;  
6                   using said control channel to relay authentication protocol messages between said  
7 creator and said requester;  
8                   if said creator can authenticate said requester, then said creator sharing a security  
9 association it holds with said requester;

10                   using said security association shared among members of said personal VLAN to  
11 identify frames originating from said members, wherein:

12                   if a received frame carries a null virtual LAN ID (VID) or is untagged,  
13 then using its source MAC address to determine a preliminary VLAN classification of said  
14 received frame; and

15                   if said received frame carries a VID, then using said VID as said  
16 preliminary VLAN classification instead;

17                   using said preliminary VLAN classification to index into a table of  
18 security associations giving an authentication code key;

19                   said received frame carrying an authentication code computed over a  
20 frame payload thereof using a message digest algorithm agreed upon by both said creator and  
21 said requester at authentication time and having been recorded in said table of security  
22 associations;

23                   a receiver of said received frame re-computing an authentication code,  
24 using said authentication code key, over said payload of said received frame;

25                   comparing said re-computed authentication code with said received  
26 authentication code;

27                   wherein if said re-computed authentication code and said received  
28 authentication code match, then said preliminary VLAN classification becomes a final VLAN  
29 classification;

30                   using said final VLAN classification as a value of a VLAN classification  
31 parameter of any corresponding data request primitives;

32                   decrypting said received frame using said security association; and  
33 submitting said decrypted frame to a forwarding and learning process;  
34 otherwise, discarding said received frame.

32-37. (Canceled)

1                   38.   (Currently amended): A method for segregating traffic among a plurality  
2 of end stations associated with a network access point comprising:

3                   an end station from among said plurality of end stations performing an initial  
4 authentication operation;  
5                   receiving a frame at said end station;  
6                   if said received frame carries a null virtual LAN ID (VID) or is untagged, then  
7 using its source MAC address to determine a preliminary VLAN classification of said received  
8 frame;  
9                   if said received frame carries a VID, then using said VID as said preliminary  
10 VLAN classification instead;  
11                  using said preliminary VLAN classification to index into a table of security  
12 associations giving a cryptographic authentication code key;  
13                  said received frame including a cryptographic authentication code computed over  
14 a frame payload thereof using a cryptographic message digest algorithm that is determined at a  
15 time during said initial authentication operation, said cryptographic message digest algorithm  
16 being recorded in said table of security associations;  
17                  said end station re-computing said cryptographic authentication code, using said  
18 cryptographic authentication code key, over said payload of said received frame;  
19                  comparing said re-computed cryptographic authentication code with said received  
20 cryptographic authentication code;  
21                  wherein if said re-computed cryptographic authentication code and said received  
22 cryptographic authentication code match, then:  
23                    using said preliminary VLAN classification as a value of a VLAN  
24 classification parameter of any corresponding data request primitives;  
25                    decrypting said received frame using said table of security associations,  
26                  and  
27                    submitting said decrypted frame to a forwarding and learning process;  
28                  wherein if said re-computed cryptographic authentication code and said received  
29 cryptographic authentication code do not match, then discarding said received frame.

1                   39.     (Previously presented): The method of claim 38 wherein said  
2 authentication code is a cryptographic authentication code which uniquely identifies a VLAN to  
3 which traffic belongs.

1                   40.     (Previously presented): The method of claim 38 wherein said  
2 authentication code key is generated during said initial authentication.

1                   41.     (Previously presented): The method of claim 38 wherein said initial  
2 authentication operation is performed between said end station and said access point.

1                   42.     (Currently amended): The method of claim 41 wherein said cryptographic  
2 message digest method ~~method~~ algorithm is agreed upon by both said access point and said end station.